OMB No. 0607-0725: Approval Expires 08/31/2004

FORM **CS-1**
(04/18/02)

2001 Computer Security Survey

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU
ACTING AS COLLECTION AGENT FOR THE
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

DUE DATE:

[Preprint due date]

RETURN COMPLETED FORM TO:

U.S. CENSUS BUREAU
1201 East Tenth Street
Jeffersonville, IN 47132

OR FAX TO:

1-888-353-4102

For assistance, call
1-800-227-1735 weekdays,
8:00 a.m. to 5:00 p.m. EDT

DRAFT, April 18

[Preprint company name here]
[Preprint company address here]

(Please correct any errors in name, address, and ZIP Code.)

NOTICE OF CONFIDENTIALITY -- Your report to the Census Bureau is confidential by law (Title 13, Section 9 of the U.S. Code). It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act, and ensures that copies of your responses are immune from legal process.

Please refer to the enclosed instructions before completing the survey.

SURVEY SCOPE -- This voluntary survey collects data on the type and frequency of computer security incidents in which a computer was used as the means of committing a crime against the company.

REPORTING PERIOD -- The reporting period for this survey is calendar year 2001. If 2001 calendar year figures are not available, please use fiscal year 2001 data.

ESTIMATES are acceptable.

Report for DOMESTIC OPERATIONS ONLY.

I. COMPUTER SECURITY CONCERNS

1. What are the top three computer security concerns for this company? Mark (X) three.

011

1 ☐ Embezzlement
2 ☐ Fraud
3 ☐ Theft of proprietary information
4 ☐ Denial of service
5 ☐ Vandalism or sabotage (electronic)
6 ☐ Computer virus
7 ☐ Other intrusion or breach of computer system
8 ☐ Misuse of computers by employees (Internet, e-mail, etc.)
9 ☐ Unlicensed copying or use of software
10 ☐ Other (specify)

II. COMPUTER INFRASTRUCTURE & SECURITY

REPORTING PERIOD -- The reporting period for this survey is calendar year 2001. If 2001 calendar year figures are not available, please use fiscal year 2001 data.

Report for DOMESTIC OPERATIONS ONLY.

2 a. In 2001, what types of computer networks did this company use? Mark (X) all that apply.

021

1 ☐ Local area network (LAN)
2 ☐ Wide area network (WAN)
3 ☐ Process control network
4 ☐ Virtual/private network (VPN)
5 ☐ Electronic data interchange (EDI)
6 ☐ Internet access
7 ☐ Intranet
8 ☐ Extranet
9 ☐ Stand alone PC (not on LAN)
10 ☐ Company has no computers *[Skip to 18, page 7.]*
11 ☐ Don't know

b. In 2001, what types of access to its networks did this company have? Mark (X) all that apply.

022

1 ☐ Wireless access to e-mail
2 ☐ Wireless access to Internet
3 ☐ Wireless access to other company networks
4 ☐ Publicly accessible website with e-commerce capabilities
5 ☐ Publicly accessible website without e-commerce capabilities
6 ☐ Other (specify)
7 ☐ None of the above
8 ☐ Don't know

3 a. In 2001, what types of computer system security technology did this company use? Mark (X) all that apply.

031

1 ☐ Anti-virus software
2 ☐ Biometrics
3 ☐ Digital certificates
4 ☐ E-mail logs/filters
5 ☐ System administrative logs
6 ☐ Encryption
7 ☐ Firewall
8 ☐ Intrusion detection system
9 ☐ One-time password generators (create single-use passwords)
10 ☐ Reusable passwords (change every 30 or 60 days, etc.)
11 ☐ Other (specify)
12 ☐ None; no computer security
13 ☐ Don't know

b. In 2001, how much did this company spend on the types of computer system security technology identified in 3a above? ESTIMATES are acceptable.

	Mil.	Thou.	Dol.
032 $			

c. In 2001, what computer security services did this company contract out to a third party? Mark (X) all that apply.

033

1 ☐ Installation of computer security
2 ☐ Monitoring of computer security
3 ☐ Evaluation of vulnerability
4 ☐ Managed computer security
5 ☐ Other (specify)
6 ☐ None; all computer security is done in-house
7 ☐ Don't know

4 a. Which statement best describes the status of any business continuity/disaster recovery programs for this company's computer systems at the end of 2001? Mark (X) only one.

041

1 ☐ A business continuity/disaster recovery program was in place
2 ☐ A business continuity/disaster recovery program was being implemented
3 ☐ A business continuity/disaster recovery program was in planning stage
4 ☐ Company had no plans for a business continuity/disaster recovery program in 2001
5 ☐ Don't know

b. If a computer system business continuity/disaster recovery program was in place, was it tested in 2001?

042

1 ☐ Yes
2 ☐ No
3 ☐ Don't know
4 ☐ Not applicable

5. In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

051

1 ☐ Yes
2 ☐ No
3 ☐ Don't know
4 ☐ Not applicable

III. UNLICENSED COPYING OR USE OF SOFTWARE

6 a. In 2001, did this company develop software for resale?

061

1 ☐ Yes
2 ☐ No---> *[If "No," skip to 7.]*

b. In 2001, did this company experience any unlicensed copying or use of software which it developed for resale?

062

1 ☐ Yes
2 ☐ No
3 ☐ Don't know

c. What was the estimated revenue lost in 2001 from this unlicensed copying or use?

	Mil.	Thou.	Dol.
063 $			

NOTICE OF CONFIDENTIALITY -- Your report to the Census Bureau is confidential by law (Title 13, Section 9 of the U.S. Code). It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and used only for statistical purposes from which no firm may be identified. See page 1 of this survey for more details.

IV. TYPES OF COMPUTER SECURITY INCIDENTS

The questions in this section pertain to computer security incidents, where the word "incident" refers to any unauthorized access, intrusion, breach, compromise or use of this company's computer system.

Computer security incidents may be committed by people either inside or outside the company and include embezzlement, fraud, theft of proprietary information, denial of service, vandalism, sabotage, computer virus, etc.

EXCLUDE unlicensed copying or misuse of software. This should be reported in question 6.

Please do NOT duplicate information. If an incident can be classified under multiple categories, report it under the FIRST applicable category. For example, if proprietary information was stolen or copied by means of computer fraud, report it under fraud and do NOT include it under theft.

ESTIMATES are acceptable.

7. EMBEZZLEMENT

Embezzlement is the unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.

INCLUDE instances in which a computer was used to wrongfully transfer, counterfeit, forge or gain access to money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by the person to whom it was entrusted.

a. Did this company detect any incidents in which any computer was used to commit embezzlement against this company in 2001?

071

1 ☐ Yes--> **How many incidents were detected?**

2 ☐ No---> *[If "No," skip to 8.]* 072 _____ Number

b. How many of these incidents of embezzlement resulted in monetary loss? 073 _____ Number

[If zero, skip to 8.]

c. What was the total monetary loss incurred in 2001 associated with these incidents?

INCLUDE actual losses such as the value of stolen information, 074 $ | Mil. | Thou. | Dol. |
|---|---|---|

stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

d. Of this amount, what was the dollar value taken by means of embezzlement? 075 $

Mil.	Thou.	Dol.

8. FRAUD

Fraud is the intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

INCLUDE instances in which a computer was used by someone inside or outside the company in order to defraud this company of money, property, financial documents, insurance policies, deeds, use of rental cars, various services, etc., by means of forgery, misrepresented identity, credit card or wire fraud, etc.

EXCLUDE incidents of embezzlement. Report these in 7.

a. Did this company detect any incidents in which any computer was used by someone inside or outside this company to commit fraud against this company in 2001?

081

1 ☐ Yes--> **How many incidents were detected?**

2 ☐ No---> *[If "No," skip to 9.]* 082 _____ Number

b. How many of these incidents of fraud resulted in monetary loss? 083 _____ Number

[If zero, skip to 9.]

c. What was the total monetary loss incurred in 2001 associated with these incidents?

INCLUDE actual losses such as the value of stolen information, 084 $ | Mil. | Thou. | Dol. |
|---|---|---|

stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

d. Of this amount, what was the dollar value taken by means of fraud? 085 $

Mil.	Thou.	Dol.

IV. TYPES OF COMPUTER SECURITY INCIDENTS (Continued)

9. THEFT OF PROPRIETARY INFORMATION

Theft of proprietary information is the illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, personal or financial information, etc., usually by electronic copying.

EXCLUDE incidents which resulted in embezzlement or fraud. Report these in 7 and 8, page 3.

EXCLUDE incidents which resulted in unlicensed use or copying of software developed by this company for resale. Report these in 6, page 2.

a. Did this company detect any incidents in which any computer was used by someone inside or outside the company in order to obtain proprietary information in 2001?

091

1 ☐ Yes--> **How many incidents were detected?**
2 ☐ No---> *[If "No," skip to 10.]* 092 _____ Number

b. How many of these incidents of theft of proprietary information resulted in monetary loss? 093 _____ Number
[If zero, skip to 10.]

c. What was the total monetary loss incurred in 2001 associated with these incidents?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
094 $			

d. Of this amount, what was the dollar value of the information taken by means of theft?

	Mil.	Thou.	Dol.
095 $			

10. DENIAL OF SERVICE

Denial of service is the disruption of an Internet connection that results in the degradation of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

a. Did this company detect any incidents of denial of service which resulted in a noticeable degradation of its Internet connection in 2001?

101

1 ☐ Yes--> **How many incidents were detected?** 102 _____ Number
2 ☐ No---> *[If "No," skip to 11.]*

b. How many of these incidents of denial of service resulted in the company taking some action to restore the level of service? 103 _____ Number
[If zero, skip to 10d, below.]

c. What was the total duration (in hours) of the incidents of denial of service indicated in 10b above?
INCLUDE downtime needed for repairs. 104 _____ Hours

d. How many of these incidents of denial of service resulted in monetary loss? 105 _____ Number
[If zero, skip to 11.]

e. What was the total monetary loss incurred in 2001 associated with these incidents?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
106 $			

f. Of this amount, how much was spent in 2001 to recover from these incidents of denial of service?
INCLUDE the cost of diagnosis, repairs and replacement such as labor, hardware, software, etc.

	Mil.	Thou.	Dol.
107 $			

IV. TYPES OF COMPUTER SECURITY INCIDENTS (Continued)

11. VANDALISM OR SABOTAGE (ELECTRONIC)

Vandalism or sabotage is the deliberate or malicious damage, defacement, destruction, or other alteration of electronic files, data, web pages, programs, etc.

EXCLUDE incidents of alteration which resulted in fraud. Report these in 8, page 3.

a. Did this company detect any incidents in which any part of its computer networks was electronically vandalized or sabotaged in 2001?

111
1 ☐ Yes--> **How many incidents were detected?** 112 _____ Number
2 ☐ No---> *[If "No," skip to 12.]*

b. How many of these incidents of vandalism or sabotage resulted in the downtime of any part of this company's networks or individual workstations?
INCLUDE downtime needed for repairs. 113 _____ Number
[If zero, skip to 11d, below.]

c. What was the total downtime of each of the following due to these acts of vandalism or sabotage?
INCLUDE downtime needed to make repairs.

1) Downtime of company networks 114 _____ Hours
2) Downtime of individual workstations
EXCLUDE network-wide downtime. 115 _____ Hours

d. How many of these incidents of vandalism or sabotage resulted in monetary loss? 116 _____ Number
[If zero, skip to 12.]

e. What was the total monetary loss incurred in 2001 associated with these incidents?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
117 $			

f. Of this amount, how much was spent in 2001 to recover from these incidents of vandalism or sabotage?
INCLUDE the cost of diagnosis, repairs and replacement such as labor, hardware, software, etc.

	Mil.	Thou.	Dol.
118 $			

g. How many of these incidents of vandalism or sabotage were caused by a virus? 119 _____ Number

12. COMPUTER VIRUS

A computer virus is a hidden fragment of computer code which propagates by inserting itself into other programs.

INCLUDE viruses, worms, Trojan horses, etc.

EXCLUDE incidents of denial of service. Report these in 10, page 4.

EXCLUDE incidents which resulted in damage, defacement or destruction of electronic files, data, web pages, programs, etc. Report these in 11.

a. In 2001, did this company detect any computer viruses before they could be executed?

121
1 ☐ Yes--> **How many times were**
2 ☐ No **unexecuted viruses detected?** 122 _____ Number
[Continue with 12b, below.]

b. Did this company detect any viruses which had been executed in any part of its computer system in 2001?
EXCLUDE viruses already reported in this survey.

123
1 ☐ Yes--> **How many times were viruses**
2 ☐ No **executed into the system?** 124 _____ Number
[If "No," skip to 13.]

c. How many times did these viruses result in downtime? 125 _____ Number
[If zero, skip to 12e, below.]

d. What was the total downtime of each of the following due to these computer viruses?
INCLUDE downtime needed for repairs.

1) Downtime of company networks 126 _____ Hours
2) Downtime of individual workstations
EXCLUDE network-wide downtime. 127 _____ Hours

e. How many times did any of these viruses result in monetary loss? 128 _____ Number
[If zero, skip to 13.]

f. What was the total monetary loss incurred in 2001 associated with these viruses?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
129 $			

g. Of this amount, how much was spent in 2001 to recover from these computer viruses?
INCLUDE the cost of diagnosis, repairs and replacement such as labor, hardware, software, etc.

	Mil.	Thou.	Dol.
120 $			

IV. TYPES OF COMPUTER SECURITY INCIDENTS (Continued)

13. OTHER COMPUTER SECURITY INCIDENTS

INCLUDE all other intrusions, breaches and compromises of this company's computer networks (such as hacking or sniffing) regardless of whether or not loss or damage was sustained as a result.

EXCLUDE incidents already reported in this survey.

a. Did this company detect any other computer security incidents in 2001?

131
1 ☐ Yes
2 ☐ No---> *[If "No," skip to 14.]*

b. Please briefly describe these types of computer security incidents.

132

c. How many of these incidents resulted in downtime? 133 ____ Number
[If zero, skip to 13e, below.]

d. What was the total downtime of each of the following due to these other computer security incidents?
INCLUDE downtime needed for repairs.

1) Downtime of company networks	134	Hours
2) Downtime of individual workstations EXCLUDE network-wide downtime.	135	Hours

e. How many of these other computer security incidents resulted in monetary loss? 136 ____ Number
[If zero, skip to 14.]

f. What was the total monetary loss incurred in 2001 associated with these incidents?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
137 $			

g. Of this amount, how much was spent in 2001 to recover from these other computer security incidents?
INCLUDE the cost of diagnosis, repairs and replacement such as labor, hardware, software, etc.

	Mil.	Thou.	Dol.
138 $			

V. SPECIFIC INCIDENT INFORMATION

For questions 14 - 17, please report for the single most significant computer security incident for this company in 2001. If there were multiple similar incidents, choose a representative incident and report for that ONE.

14a. In 2001, when did this company's single most significant computer security incident occur? 1 Month Year 141 ____ / ____

b. Which of this company's computer networks were affected in this particular incident?
Mark (X) all that apply.

142

1 ☐ Local area network (LAN)
2 ☐ Wide area network (WAN)
3 ☐ Process control network
4 ☐ Virtual/private network (VPN)
5 ☐ Electronic data interchange (EDI)
6 ☐ E-mail system
7 ☐ Internet access
8 ☐ Intranet
9 ☐ Extranet
10 ☐ Individual workstation (on LAN)
11 ☐ Stand-alone PC (not on LAN)
12 ☐ Other (specify)
13 ☐ Don't know
14 ☐ Not applicable

c. If this particular incident resulted in any downtime, what was the total duration (in hours) of each of the following?
INCLUDE downtime needed for repairs.

1) Downtime of company networks Exclude denial of service to the Internet.	143	Hours
2) Downtime of individual workstations EXCLUDE network-wide downtime.	144	Hours
3) Denial of Service to Internet connection	145	Hours

d. What was the total monetary loss incurred in 2001 associated with this incident?
INCLUDE actual losses such as the value of stolen information, stolen or damaged property, forged financial documents, etc., and the cost of labor, hardware, software, etc., necessary to diagnose the problem, repair or replace components, etc. If possible, include the estimated value of downtime, lost productivity, income from lost sales, labor or fees for legal or investigative work, etc.

	Mil.	Thou.	Dol.
146 $			

e. Of this amount, what was the dollar value taken by theft in this particular incident?

	Mil.	Thou.	Dol.
147 $			

f. Of the total in 14d above, how much was spent in 2001 to recover from this particular incident?
INCLUDE cost of labor, hardware, software, etc. needed to repair damage, get back online, etc.

	Mil.	Thou.	Dol.
148 $			

g. Which of the following types describes this particular incident? Mark (X) only one.

149

1 ☐ Embezzlement
2 ☐ Fraud
3 ☐ Theft of proprietary information
4 ☐ Denial of service
5 ☐ Vandalism or sabotage (electronic)
6 ☐ Computer virus
7 ☐ Other intrusion or breach
8 ☐ Other (specify)
9 ☐ Not applicable

V. SPECIFIC INCIDENT INFORMATION (Continued)

15 a. What was the relationship between the suspected offender and this company at the time of this particular incident? Mark (X) only one.
If there were multiple offenders, answer for the one viewed as the principal offender.
151
1 ☐ Current employee, contractor, temporary worker, etc.
2 ☐ Former employee, contractor, temporary worker, etc.
3 ☐ Domestic competitor
4 ☐ Foreign competitor, foreign hacker, other foreign entity (specify country)
5 ☐ Hacker/cracker (no known association with this company)
6 ☐ Other (specify)
7 ☐ Don't know

b. Which of the following were used by the suspected offender to access this company's networks in this particular incident? Mark (X) all that apply.
152
1 ☐ Hardwired communications lines
2 ☐ Wireless access to e-mail
3 ☐ Wireless access to Internet
4 ☐ Wireless access to other company networks
5 ☐ Publicly accessible website with e-commerce capabilities
6 ☐ Publicly accessible website without e-commerce capabilities
7 ☐ Other (specify)
8 ☐ None of the above
9 ☐ Don't know
10 ☐ Not applicable

16. To whom was this incident reported?
Mark (X) all that apply.
161
1 ☐ Local law enforcement
2 ☐ State law enforcement
3 ☐ Federal Bureau of Investigation
4 ☐ Federal Computer Incident Response Center
5 ☐ Other Federal agency (specify)
6 ☐ CERT ® Coordination Center
7 ☐ Information Sharing and Analysis Center (ISAC)
8 ☐ System Administration, Networks, and Security Institute (SANS)
9 ☐ Internet Service Provider (ISP)
10 ☐ Did not report outside the company
11 ☐ Other (specify)

17. If this incident was not reported outside the company, what were the reasons? Mark (X) all that apply.
171
1 ☐ Negative publicity
2 ☐ Lower customer/client/investor confidence
3 ☐ Competitor advantage
4 ☐ Did not want data/hardware seized as evidence
5 ☐ Did not know who to contact
6 ☐ Incident outside jurisdiction of law enforcement
7 ☐ Nothing to be gained/nothing worth pursuing
8 ☐ Other (specify)

VI. COMPANY INFORMATION

18 a. Which line of business most closely corresponds to this company's primary activity in 2001?
Mark (X) only one.
181
1 ☐ Accounting, Bookkeeping, Payroll and Tax Preparation Services
2 ☐ Administration and Support Services, and Waste Management and Remediation Services
3 ☐ Advertising and Related Services
4 ☐ Agriculture (Crop and Animal Production)
5 ☐ Architectural, Engineering and Related Services
6 ☐ Arts; Entertainment; Recreation
7 ☐ Computer Systems Design; Specialized Design; Related Services
8 ☐ Construction
9 ☐ Data Processing, Hosting and Related Services
10 ☐ Educational Services
11 ☐ Finance
12 ☐ Forestry, Fishing & Hunting
13 ☐ Health Care Services (includes Physicians; Hospitals; Nursing and Residential care)
14 ☐ Insurance Carriers and Related Activities; Funds, Trusts and Other Financial Vehicles
15 ☐ Internet Publishing and Broadcasting
16 ☐ Internet Service Providers (ISP's); Web Search Portals
17 ☐ Legal Services
18 ☐ Management of Companies & Enterprises
19 ☐ Manufacturing of Durable Goods
20 ☐ Manufacturing of Non-Durable Goods
21 ☐ Mining; Quarrying; Oil & Gas Extraction; Related Support Activities
22 ☐ Motion Picture and Sound Recording Industries
23 ☐ News Syndicates, Libraries, Archives & Similar Information Services
24 ☐ Publishing and Broadcasting Industries (except Internet)
25 ☐ Real Estate; Rental and Leasing Services (includes Rental and Leasing of Tangible Goods)
26 ☐ Retail Trade
27 ☐ Scientific Research and Development Services; Management, Scientific, and Technical Consulting Services; Other Professional, Scientific and Technical Services
28 ☐ Social Assistance/Services
29 ☐ Transportation (includes Pipelines & Couriers); Support Activities
30 ☐ Traveler Accommodation and Food Services
31 ☐ Telecommunications Services
32 ☐ Utilities
33 ☐ Warehousing and Storage
34 ☐ Wholesale Trade
35 ☐ Miscellaneous Services, not elsewhere classified, such as Repair, Maintenance, Personal, Laundry and Similar Services; Civic Grantmaking, Professional, Religious and Similar Organizations
36 ☐ Other (specify)

VI. COMPANY INFORMATION (Continued)

18 b. Please briefly describe this company's business activities.

Primary activity:

182

Secondary activities:

183

c. What were the total sales, receipts, and operating revenue (net of returns and allowances, and excise and sales taxes) for this company in 2001?

	Bil.	Mil.	Thou.	Dol.
184 $				

d. What was the total number of employees ON THIS COMPANY'S PAYROLL for the pay period which includes March 12, 2001?

Count EACH part-time employee as one.
Exclude contractors, leased and temporary employees.

185 _____ Number

19. Do the data reported in this survey cover the calendar year 2001?

191

1 ☐ Yes
2 ☐ No --> Specify period covered:

3 Month Year FROM ____/____ 4 Month Year TO ____/____

20. What was this company's operational status at the end of 2001? Mark (X) only one.

201

1 ☐ In operation
2 ☐ Under construction, development, or exploration
3 ☐ Temporarily or seasonally inactive
4 ☐ Ceased operation
5 ☐ Sold or leased to another operator

6 Month Year ____/____

Successor Company:

Name

Street Address

City State Zip

CONTACT INFORMATION

Person to contact regarding this report:

Name

Title

( ) - Ext.
Phone

( ) - Ext.
Fax

E-mail address

REMARKS

999 (Please use this space for any explanations that may be essential in understanding your reported data.)